CLAIMS:

1. (currently amended) A method of implementing Internet protocol security in a mobile IP network, comprising the steps of:

initiating communication from by a first node to a second node via the mobile IP network;

checking searching by the first node a cache thereof to see if any security association is established with the second node; and

initiating by the first node establishment of a security association for protecting communications with the second node if no security association is established with the second node without waiting for a response communication from the second node.

- 2. (original) A method as recited in claim 1, wherein the second node is a mobile node situated away from its home link.
- 3. (original) A method as recited in claim 2, wherein the first node initiates communication with the second node by sending a control packet to the second node through the second node's home agent and the second node in response returns a binding update to the first node.
- 4. (original) A method as recited in claim 1, wherein the security association established employs a Kerberos key exchange method.
- 5. (original) A method as recited in claim 4, wherein at least one of the first and second nodes uses a secret key established in Layer 2 for Layer 3 authentication.
- 6. (original) A method as recited in claim 1, wherein the network has security association managers, and the security association is established by the security association managers.
- 7. (currently amended) A method as recited in claim 1, wherein <u>at least one</u> <u>of the first and second nodes have has a subscriber identification module, and the security association established is stored in the subscriber identification module.</u>

- 8. (original) A method as recited in claim 1, wherein the security association has a long lifetime and is used over multiple sessions of communications between the first and second nodes.
- 9. (original) A method as recited in claim 1, wherein the communication is a real-time interactive digital data communication.
- 10. (original) A method as recited in claim 9, wherein the real-time interactive digital data communication is voice over Internet protocol.
- 11. (original) A method as recited in claim 1, wherein the network complies with International Mobile Telecommunications-2000 standards.
- 12. (currently amended) A method for implementing Kerberos-based Internet security protocol in a mobile IP network, comprising the steps of:

establishing a Layer 2 secret key between a <u>first</u> node and a base transceiver station when the <u>first</u> node is establishing wireless connection with the base transceiver station; <u>and</u>

reporting the established Layer 2 secret key from a Layer 2 to a Layer 3 in the node; and

using the <u>reported_established</u> Layer 2 secret key to <u>authenticate_establish</u> <u>a security association for layer 3 communication via the mobile IP network between the</u> fist node to the network when the node logs in the network and a second node.

- 13. (currently amended) A method as recited in claim 12, wherein the <u>layer 3</u> communication is a real-time interactive digital data communication.
- 14. (original) A method as recited in claim 13, wherein the real-time interactive digital data communication is voice over Internet protocol.
- 15. (original) A method as recited in claim 12, wherein the network complies with International Mobile Telecommunications-2000 standards.

16-21. (cancelled)

- 22. (new) A method as recited in claim 1, wherein the first node initiates establishment of a security association for protecting communications with the second node, if no security association with the second node is found in the cache.
- 23. (new) A mobile terminal configured to implement Internet protocol security in a mobile IP network, comprising:

a cache configured to store security associations established with corresponding nodes;

a communication control that initiates communication to a second node via the mobile IP network;

a security association locator that searches the cache to see if any security association is established with the second node; and

a security association control that initiates establishment of a security association for protecting communications with the second node without waiting for a response communication from the second node.

- 24. (new) A mobile terminal as recited in claim 23, wherein the second node is a mobile node situated away from its home link.
- 25. (new) A mobile terminal as recited in claim 24, wherein the communication control initiates communication with the second node by sending a control packet to the second node through the second node's home agent and the second node in response returns a binding update to the mobile terminal.
- 26. (new) A mobile terminal as recited in claim 23, wherein the security association established employs a Kerberos key exchange method.
- 27. (new) A mobile terminal as recited in claim 26, wherein at least one of the mobile terminal and second nodes uses a secret key established in Layer 2 for Layer 3 authentication.
- 28. (new) A mobile terminal as recited in claim 23, wherein the network has security association managers, and the security association is established by the security association managers.

- 29. (new) A mobile terminal as recited in claim 23, wherein at least one of the mobile terminal and the second node has a subscriber identification module, and the security association established is stored in the subscriber identification module.
- 30. (new) A mobile terminal as recited in claim 23, wherein the security association has a long lifetime and is used over multiple sessions of communications between the mobile terminal and the second node.
- 31. (new) A mobile terminal as recited in claim 23, wherein the communication is a real-time interactive digital data communication.
- 32. (new) A mobile terminal as recited in claim 31, wherein the real-time interactive digital data communication is voice over Internet protocol.
- 33. (new) A mobile terminal as recited in claim 23, wherein the network complies with International Mobile Telecommunications-2000 standards.
- 34. (new) A mobile terminal as recited in claim 23, wherein the security association control initiates establishment of a security association for protecting communications with the second node, if no security association with the second node is found in the cache.